

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

- 1 1. (Currently amended): A tamper-resistant computer system having a CPU
2 and a main memory for executing application software, comprising:
3 a first operating system; and
4 a second operating system;
5 wherein the application software comprises a first component program executed
6 by the first operating system, and a second component program executed by the second operating
7 system, wherein the first component program has a user interface for receiving an operational
8 instruction from a user of the computer system and for issuing a command to the second
9 component program, and
10 wherein the second component program selectively performs the command issued
11 by the first component program if execution thereof has been designated as permitted in advance,
12 thereby preventing the second component program from being accessed by the user.
- 1 2. (Original): A tamper-resistant computer system as claimed in claim 1,
2 further comprising a communication control program that sends a command issued by the first
3 component program to the second component program if execution thereof is permitted.
- 1 3. (Original): A tamper-resistant computer system as claimed in claim 2,
2 further comprising a multi-OS control program for controlling the first and second operating
3 systems;
4 wherein the multi-OS control program establishes a particular region in a memory
5 area managed by the first operating system so that the particular region can be referred to by the
6 communication control program, wherein the user interface of the first component program
7 writes the command into the particular region for issuance thereof, and

8 wherein, by referring to the particular region, the communication control program
9 reads a command stored in the particular region by the first component program, and then, by
10 making reference to a list of the permitted commands held in a memory area managed by the
11 second operating system, the communication control program sends the command to the second
12 component program if the command is in the list.

1 4. (Original): A tamper-resistant computer system as claimed in claim 3
2 further including a tamper-resistant hardware module for storing a system boot program;
3 wherein the tamper-resistant computer system includes an initial program for
4 reading the system boot program at system startup,
5 wherein the system boot program includes a function for executing the multi-OS
6 control program, and wherein the multi-OS control program includes a function for executing the
7 first and second operating systems.

1 5. (Original): A tamper-resistant computer system as claimed in claim 4,
2 wherein the second component program comprises a system boot program,
3 cryptographic software, and digital signature, wherein the hardware module includes a
4 decryption key for the cryptographic software and a function for authenticating the system boot
5 program,
6 wherein the system boot program includes a function for performing
7 authentication for the hardware module, a function for extracting the decryption key for the
8 cryptographic software from the hardware module, and a function for decrypting the
9 cryptographic software with the decryption key extracted from the hardware module, and
10 wherein, according to a command from the first component program, the system
11 boot program is executed, and in response the cryptographic software is decrypted and executed.

1 6. (Original): A tamper-resistant computer system as claimed in claim 5
2 wherein the hardware module further includes a decryption key for cryptographic data to be used
3 by the second component program, and wherein the second component decrypts the
4 cryptographic data.

1 7. (Original): A tamper-resistant computer system as claimed in claim 3,
2 wherein, at start of the second component program, the second component
3 program adds a command permitted for the first component program to the list of permitted
4 commands, and
5 wherein, at the time of termination of the second component program, the second
6 component program removes the command from the list of permitted commands.

1 8. (Original): A tamper-resistant computer system as claimed in claim 1,
2 wherein the second component program comprises a command processing program for
3 command execution, and a communication control program through which a command issued by
4 the first component program is sent to the command processing program if execution thereof is
5 permitted.

1 9. (Original): A method for installing system software onto a tamper-
2 resistant computer system comprising:
3 providing an installation program for system software which includes an
4 installation start program, a cryptographic system file, and a digital signature, and wherein the
5 installation start program includes a function for extracting a decryption key for the
6 cryptographic system file from the hardware module and a function for decrypting the
7 cryptographic system file with the decryption key extracted from the hardware module; and
8 executing the installation start program; and decrypting the cryptographic system
9 file.

1 10. (Original): A method as in claim 9, wherein the method further
2 comprises:
3 providing an installation program for application software which installation
4 program includes a first installation program executed by a first operating system and a second
5 installation program executed by a second operating system; wherein the first installation
6 program includes a function for writing a first component program into a memory area managed

7 by the first operating system and a function for calling the second installation program, wherein
8 the second installation program has a function for writing the second component program into a
9 memory area managed by the second operating system;
10 executing the first installation program;
11 calling the second installation program; and
12 executing the second installation program.

1 11. (Original): A method as in claim 9, wherein the installation program for
2 the application software includes a digital signature, and a step is performed of checking the
3 digital signature before writing the first and second component programs into the memory areas.

1 12. (New): A tamper-resistant computer system having a CPU and a main
2 memory for executing application software, comprising:
3 a first operating system;
4 a second operating system;
5 a first application-level program executing on the first operating system; and
6 a second application-level program executing on the second operating system,
7 wherein the first application-level program has a user interface for receiving an
8 operational instruction from a user of the computer system,
9 wherein the first application-level program is configured to issue a command to
10 the second component program in response to input received by the user interface,
11 wherein the second application-level program performs the command issued by
12 the first component program if execution thereof has been designated as permitted in advance,
13 thereby preventing the second component program from being accessed by the user.